Software Release Note

1.1 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP v4.1 for bug fixes.

1.2 Software Release Details

Date	October 31, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.22.31	Defect Fix Release

1.3 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIPv4.1	Firmware Release	4.1.22.31	Release firmware contains following • Defect Fixes (Bugs detail are mentioned in table 1.11.1). • Updated MO files for FR-903160068 are included. • Updated 3CtoDT700languagemappings.txt for T-30470 is included. • Updated dt-austria.cfg, dt-belgium.cfg and dt-switzerland.cfg for T-30450,T-30451 and T-30452 are included. • Updated dt-000000000000-sip.cfg for FR-001170125, FR-903160068 and FR-903170047 is included.	

1.4 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.5 List of Fixed Issue

1.5.1 List of Fixed Issue in STD-SIP 4.1.22.31

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	FR-903170047 (STSI-1206)	Defect	DT820 phone with configured 802.1x restarts after unplugging PC connected to PC port.	External	
2	FR-001170129 (STSI-1133)	Defect	Speakerphone muting a call from AT&T meeting solution is not effective until they press "1" to join a conference	External	
3	FR-001170125 (STSI-1137)	Defect	While receiving group call from 3C UCM, group information is not displayed.	External	
4	FR-903160068 (STSI-1134)	Defect	Customer is asking how to disable call history feature.	External	
5	STSI-1160	Defect	Time Stamp information in SIP PUBLISH message is not UTC.	External	
6	STSI-1161	Defect	Event header is not included in SIP PUBLISH message from DT terminal. SIP PUBLISH message must contain “Event: vq-rtcpxr” header in order to identify it as RTCP-XR packet.	External	
7	STSI-1164	Defect	When RTP Payload types (PT) is “dynamic” (96~), SIP PUBLISH doesn’t	External	

			include the payload description (PD) in SessionDesc.		
8	T-30450,T-30451, T-30452	Defect	Modifying Telephony Area PSTN Numbers for Austria, Belgium and Switzerland	External	This is merge from v2.3.
9	T-30470	Defect	Change the language tags for some country entries	External	This is merge from v2.3.
10	ECR-2742	Defect	New Call History Logoff Persistence setting to allow persistent in flash only	External	This is merge from v2.3.
11	STSI-849	Defect	CRL certificate revoke not working for more than one certificate	Internal	No code change is required for this issue. This is an environmental issue.

1.6 Open Issue

The following issues have NOT been repaired in this firmware release. ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
--	STSI-786	**L2TP Connect Failed" is received for ikev1 when VPN is connected from Remote location (Behind NAT)**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.
FR-903160051	STSI-836	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.

FR-903160069	STSI-832	**DT7xx: Display Diversion destination i.c.o. activated diversion**	Maintenance Enhancement Request	This is a feature request.
--	STSI-956	**Emergency number and 11 digit number is not dialed immediately.**	Internal	This issue has been raised internally while testing localization changes for STSI-979.
--	STSI-985	**When Menu key is pressed on DT820 6D, the incorrect indication is displayed on LCD. Only the text of soft key 3 is displayed. Please see the attached photo.**	External	
	STSI-1127	**DHCP Option 120 is not supported DT820, DT730CG/DG Terminal**	Internal	
FR-903170035		**DT820 VPN lacks compatibility with VPN server equipment**	External	
AR-903170007		**Also accept general proper format for 802.1x certificates**	External	
	STSI-1132	**Different behavior is observed as compare to v2.3 during IP dialing conference issue**	Internal	
FR-903170058		**SRTP negotiation wrong DT820 returns 2 times AVP instead of SAVP**	External	
FR-927170001		**Boot Server setting is not saved properly after FW conversion.**	External	
FR-001170151		**On Univerge Blue deployment under certain unknown conditions a test DT820 phone stopped registering.**	External	
FR-001170131		**"IF user has changed ringtone and gets direct call phone plays that ringtone, however when it gets call from AA then it plays default ring tone. Customer is not using distinctive ringtone."**	External	

4.1.20.29 Release

1.7 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP v4.1 for bug fixes.

1.8 Software Release Details

Date	August 29, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.20.29	Defect Fix Release

1.9 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIPv4.1	Firmware Release	4.1.20.29	Release firmware contains following • Defect Fixes (Bugs detail are mentioned in table 1.11.1).	

1.10 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.11 List of Fixed Issue

1.11.1 List of Fixed Issue in STD-SIP 4.1.20.29

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	AR-927170003 (STSI-1128) (STSI-1130) (STSI-1085)	Defect	DT phone will stop sending RTP when negotiating srtp	External	STSI- 1085 is currently not visible in JIRA. It is added in list because STSI- 1085 is marked as open issue in 4.1.19.7 release.
2	STSI-1129/ STSI-1083	Defect	Terminal moves to Acquired state instead of held when invalid client cert password is provided.	Internal	STSI-1083 is currently not visible in JIRA. It is added in list because STSI- 1083 is marked as open issue in 4.1.19.7 release.
3	STSI-1106	Defect	When ClientCert file is not given instead of showing parameter missing state it goes to Held State	Internal	
4	FR-001170119 (STSI-1131)	Invalid Defect	DT820 6Key are constantly rebooting after enabling "Giga". Phones were just working fine when "giga" was disabled.	External	This was not a terminal side issue and didn't required any code changes.

1.12 Open Issue

The following issues have NOT been repaired in this firmware release. ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
	STSI-849	**CRL certificate revoke not working for more than one certificate**	Internal	
--	STSI-786	**L2TP Connect Failed" is received for ikev1 when VPN is connected from Remote location (Behind NAT)**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.
FR-903160051	STSI-836	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.

FR-903160068	STSI-831	**Customer is asking how to disable call history feature**	Maintenance Enhancement Request	This is a feature request.
FR-903160069	STSI-832	**DT7xx: Display Diversion destination i.c.o. activated diversion**	Maintenance Enhancement Request	This is a feature request.
--	STSI-956	**Emergency number and 11 digit number is not dialed immediately.**	Internal	This issue has been raised internally while testing localization changes for STSI-979.
--	STSI-985	**When Menu key is pressed on DT820 6D, the incorrect indication is displayed on LCD. Only the text of soft key 3 is displayed. Please see the attached photo.**	External	
FR-903170047		**DT820 phone with configured 802.1x restarts after unplugging PC connected to PC port**	External	
	STSI-1127	**DHCP Option 120 is not supported DT820, DT730CG/DG Terminal**	Internal	
FR-903170035		**DT820 VPN lacks compatibility with VPN server equipment**	External	
AR-903170007		**Also accept general proper format for 802.1x certificates**	External	
	STSI-1132	**Different behavior is observed as compare to v2.3 during IP dialing conference issue**	Internal	

4.1.19.7 Release

1.13 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP v4.1 for bug fixes.

1.14 Software Release Details

Date	July 07, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.19.7	Defect Fix Release

1.15 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIPv4.1	Firmware Release	4.1.19.7	Release firmware contains following • Defect Fixes (Bugs detail are mentioned in table 1.17.1). • Configuration file “dt-germany.cfg” is modified for T-30238 and file “dt-000000000000-sip.cfg” is modified for FR-607170001.	

1.16 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.17 List of Fixed Issue

1.17.1 List of Fixed Issue in STD-SIP 4.1.19.7

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	FR-927170002 (STSI-1059)	Defect	Phone no sending or playing RTP	External	
2	FR-001170099 (STSI-1060)	Defect	In UCAAS deployment customer phone ends up sending INVITE to private IP address of MGC instead of sending it to IP addressed where it sends general INVITE as a result of Refer-To header having private IP address.	External	
3	FR-607170001 (STSI-1062)	Defect	The Led of the Speaker + Mic + line is ON + dial tone is given, The caller starts dialing and tone disappear as if the call is processing but in reality the terminal is still STD.BY and it stays like this (going NOWHERE) as if you are really making a call, when pushing speakerphone key. The caller at the end has the perception that call is processing but the terminal is still on STD and at the end looks like the call fail. Steps are: 1. do not press speaker. 2. Dial any number (internal or external) 3. The speaker and mic keys are lit but the call never progresses.	External	

4	FR-607170002 (STSI-1063)	Defect	Generate Dialtone when the TrunkDial key is used on a DT-terminal	External	
5	T-30176 (STSI-998)	Defect	802.1X certificates details are not displayed properly after moving the status option under Admin settings in the terminal	External	
6	FR-903170028 (STSI-1025)	Defect	802.1x with EAP-TLS gives 802.1x : Invalid Certificate	External	
7	T-30238 (STSI-1084)	Defect	The dial tone played for German setting is incorrect	External	This is merge from v2.3.

1.18 Open Issue

The following issues have NOT been repaired in this firmware release. ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
	STSI-849	**CRL certificate revoke not working for more than one certificate**	Internal	
--	STSI-786	**L2TP Connect Failed" is received for ikev1 when VPN is connected from Remote location (Behind NAT)**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.
FR-903160051	STSI-836	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.

FR-903160068	STSI-831	**Customer is asking how to disable call history feature**	Maintenance Enhancement Request	This is a feature request.
FR-903160069	STSI-832	**DT7xx: Display Diversion destination i.c.o. activated diversion**	Maintenance Enhancement Request	This is a feature request.
--	STSI-956	**Emergency number and 11 digit number is not dialed immediately.**	Internal	This issue has been raised internally while testing localization changes for STSI-979.
--	STSI-985	**When Menu key is pressed on DT820 6D, the incorrect indication is displayed on LCD. Only the text of soft key 3 is displayed. Please see the attached photo.**	External	
--	STSI-1083	**Terminal moves to Acquired state instead of held when invalid client cert password is provided.**	Internal	This issue has been raised internally while testing changes for FR-903170028.
	STSI-1085	**RTP Packets not received for certain calls.**	External	

4.1.17.25 Release

1.19 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP v4.1 for bug fixes. This firmware is to be released for 3C as official STD-SIP v4.1 firmware. This firmware is to be released for SIP@Net as alpha test firmware.

1.20 Software Release Details

Date	May 25, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.17.25	Defect Fix Release

1.21 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIPv4.1	Firmware Release	4.1.17.25	Release firmware contains following • Defect Fixes (Bugs detail are mentioned in table 1.23.1) • New configuration files “dt-austria.cfg”, ”dt-belgium.cfg” and “dt-switzerland.cfg” are added for three EMEA countries for supporting localization (Austria, Belgium, and Switzerland). • Existing configuration files “dt-germany.cfg”, “dt-000000000000-sip.cfg” and “3CtoDT700languagemappings.txt” are modified. • Two new MO files “de_CH.mo” and “de_AT.mo” are added for EMEA countries Switzerland and Austria. • A new wav file “silentring.wav” is added in firmware package. • Xl2tpd upgrade to version 1.3.7.	

1.22 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.23 List of Fixed Issue

1.23.1 List of Fixed Issue in STD-SIP 4.1.17.25

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	FR-001160172 (STSI-975)	Defect	The DT820 will ring itself and show its extension as callerID after the user terminates a parked call scenario	External	
2	FR-903170014 (SITD-529)	Defect	VLAN tagging when set manually on the DT820 does not seem to work	External	This issue is fixed with the fix applied for FR-903170023.
3	FR-903170023 (STSI-982)	Defect	Problems during the installation of DT820 (STD SIP) on CISCO The issue seems to be related to VLAN tagging. The trace file made on the same port with a DT820 does not show any traffic for the DT820. For the DT730 there is proper trace information. So the question is why is that? Will a wrong VLAN tag result in an empty trace file when a monitor port is applied?	External	
4	FR-001170036 (STSI-978)	Defect	DT730G and DT820 firmware does not append MAC address to syslog making it impossible to segregate logs	External	

5	FR-903170016 (STSI-977)	Defect	DT730 phones work with DT-macaddress.cfg instead of DT–ext.cfg after update of phone	External	
6	FR-903170018 (STSI-976)	Defect	DT730G stops doing TFTP after 2 minutes when TFTP responses are slow	External	
7	T-29705 (STSI-980)	Defect	Add “Silent Ring” option in DT700	External	Merge from v2.3
8	STSI-979 (P:2711)	Defect	Addition of the three new country and language templates (Austria, Belgium, and Switzerland)	External	Merge from v2.3
9	T-29348 (STSI-981)	Defect	Request to update the default list of languages on the DTERM (English-Australia is removed from the default list and replaced by French-France.)	External	Merge from v2.3
10	FR-001170038	Defect	On UCaaS deployment we see that phone stopped responding to NOTIFY requests.	External	No fix has been applied for this issue as from terminal’s perspective it was behaving correctly.
11	FR-001170039	Defect	DT820 sends incorrect SUBSCRIBE. All SUBSCRIBE are supposed to be sent at 48 mins i.e. 80% of 60 mins however phone is sending after 25 mins	External	No fix has been applied for this issue as from terminal’s perspective it was behaving correctly.
12	STSI-1022	Defect	Enhancement - XL2TPD upgrade on v4.1	Internal	Xl2tpd is upgraded to version 1.3.7.
13	STSI-862	Defect	STD-SIP_v4.1: Terminal is unable to connect l2tp with gateway.	Internal	
14	STSI-983	Defect	DNS information is added to Syslog. (STD-SIP-v4.1:Univerge Blue: Two phones in Sanko USA are getting into RS_NEVER_REGISTER state)	External	The following DNS server error/information logs is added to the existing "log.level.cc" for SIP. 1. List all DNS servers learnt by phone from DHCP and/or static. 2. Query timeouts reported per learnt DNS IP address. 3. Actual DNS response as seen in Wireshark.(at log level 7)
15	FR-001170027 (STSI-1023)	Defect	On Univerge Blue cloud hosting we are seeing that random phones start	External	Merge from v2.3.

			swinging registration between two entries in SRV records		(Only one part of this issue is fixed) This fix is that, terminal will re-subscribe once the terminal will identify that source port is changed in the transport.
16	STSI-997	Defect	Inconsistency in language (Checked for Austrian vs Italian and Austrian vs German)	Internal	

1.24 Open Issue

The following issues have NOT been repaired in this firmware release. ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
	STSI-849	**CRL certificate revoke not working for more than one certificate**	Internal	
--	STSI-786	**L2TP Connect Failed" is received for ikev1 when VPN is connected from Remote location (Behind NAT)**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.
FR-903160051	STSI-836	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.

FR-903160068	STSI-831	**Customer is asking how to disable call history feature**	Maintenance Enhancement Request	This is a feature request.
FR-903160069	STSI-832	**DT7xx: Display Diversion destination i.c.o. activated diversion**	Maintenance Enhancement Request	This is a feature request.
FR-607170001	-	**LED on when using on–hook dialling**	Maintenance Enhancement Request	This is a feature request.
FR-607170002	-	**Generate Dialtone when the TrunkDial key is used on a DT–terminal**	Maintenance Enhancement Request	This is a feature request.
--	STSI-956	**Emergency number and 11 digit number is not dialed immediately.**	Internal	This issue has been raised internally while testing localization changes for STSI-979.
--	STSI-985	**When Menu key is pressed on DT820 6D, the incorrect indication is displayed on LCD. Only the text of soft key 3 is displayed. Please see the attached photo.**	External	
FR-903170028	STSI-1025	**802.1x with EAP-TLS gives 802.1x : Invalid Certificate**	External	
T-30176	STSI-998	**802.1X certificates details are not displayed properly after moving the status option under Admin settings in the terminal**	External	
FR-927170002		**Phone no sending or playing RTP**	External	

4.1.14.27 Release

1.25 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP-v4.1 for bug fix of VPN and 802.1X EAP-TLS feature.

1.26 Software Release Details

Date	February 27, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.14.27	Defect Fix Release

1.27 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIPv4.1	Firmware Release	4.1.14.27	• Bug fix for VPN feature as mentioned in section 1.29.1 • QAC warning removal code changes	

1.28 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.29 List of Fixed Issue

1.29.1 List of Fixed Issue in STD-SIP 4.1.14.27

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	AR-903170003 (STSI-850)	Defect	DT820 can hardly be reset when the SNTP server cannot be found.	External	**Following VPN connection error timers are increased from 30 Seconds to 180 seconds** ➢ **Parameter Missing (VPN).** ➢ **IPsec Connect Failed.** ➢ **L2TP Connect Failed.** ➢ **VPN Gateway Not Found.** ➢ **Certificate Expired.** ➢ **Invalid Certificate.** **VPN connection timeout is increased from 30 seconds to 60 seconds. SNTP connection timeout is also increased to 180 seconds.**
2	AR-903170004 (STSI-851)	Defect	DT820 reboots when reading out the 802.1x Publisher	External	
3	AR-903170005 (STSI-852)	Defect	DT820 with manual NTP server set does no NTP when VPN is needed	External	**This was an environment issue and no fix has been applied for fixing this issue.**

4	STSI-853	Defect	Root certificate begin information not displayed when scrolling down if client certificate is not available but displayed when scrolled up	Internal	

1.30 Open Issues

The following issues have NOT been repaired in this firmware release. ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
	STSI-849	**CRL certificate revoke not working for more than one certificate**	Internal	
--	STSI-786	**L2TP Connect Failed" is received for ikev1 when VPN is connected from Remote location (Behind NAT)**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.
FR-903160051	STSI-836	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.

FR-903160068	STSI-831	**Customer is asking how to disable call history feature**	Maintenance Enhancement Request	This is a feature request.
FR-903160069	STSI-832	**DT7xx: Display Diversion destination i.c.o. activated diversion**	Maintenance Enhancement Request	This is a feature request.

4.1.14.13 Release

1.31 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP-v4.1 for bug fix of VPN feature.

1.32 Software Release Details

Date	February 13, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.14.13	Beta Release for NECECT and NECAM Defect Fix Release for NECU

1.33 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIP v4.1	Firmware Release	4.1.14.13	• Bug fix for VPN feature as mentioned in section 1.35.1	

1.34 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.35 List of Fixed Issue

1.35.1 List of Fixed Issue in STD-SIP 4.1.14.13

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	**STSI-828**	Defect	DT820 does not connect to HTTPS boot server over VPN(RSA)	External	
2	**---**	Defect	VPN doesn’t work after upgrading to 4.1.14.7	External	

1.36 Open Issues

The following issues have NOT been repaired in this firmware release. ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
AR-903170003	STSI-850	**DT820 can hardly be reset when the SNTP server cannot be found**	External	
AR-903170004	STSI-851	**AR-903170004 -DT820 reboots when reading out the 802.1x Publisher**	External	
AR-903170005	STSI-852	**DT820 with manual NTP server set does no NTP when VPN is needed**	External	
	STSI-849	**CRL certificate revoke not working for more than one certificate**	Internal	
--	STSI-786	**L2TP Connect Failed" is received for ikev1 when VPN is connected from Remote location (Behind NAT)**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.

--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.
FR-903160051	STSI-836	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.
FR-903160068	STSI-831	**Customer is asking how to disable call history feature**	Maintenance Enhancement Request	This is a feature request.
FR-903160069	STSI-832	**DT7xx: Display Diversion destination i.c.o. activated diversion**	Maintenance Enhancement Request	This is a feature request.

4.1.14.7 Release

1.37 Scope of the Delivery

DT820 Terminal firmware beta release of STD-SIP-v4.1 for VPN and 802.1X (EAP-TLS) features.

1.38 Software Release Details

Date	February 7, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.14.7	Beta Release for US Alpha Release for EMEA

1.39 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIP v4.1	Firmware Release	4.1.14.7	• Bug fixes for VPN and 802.1X EAP-TLS as mentioned in section 1.41.1 • MO file is updated for fixing FR-903170001	

1.40 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.41 List of Fixed Issues

1.41.1 List of Fixed Issues in STD-SIP 4.1.14.7

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	FR-927160002 (STSI-833)	Defect	In the current implementation, only 503 and 580 were pulled out to play a tone (busy/reorder) in 5xx codes by phone	External	As per the applied fix, Reorder tone will not be played for response code 500. Reorder tone will only be played if there is a single call on terminal for which terminal receives 4XX to 6XX response.
2	FR-903170001 (STSI-834)	Defect	Customer requests improvement on the Dutch translations	External	nl_NL.mo file is updated for fixing this issue
3	FR-001160199 (STSI-835)	Defect	After an extension places two incoming calls on hold the next calls to the ext will not have voice	External	Merge from v2.3
4	STSI-763	Defect	Terminal is unable to download config files when VPN is connected from remote location (public network)	Internal	
5	STSI-764	Defect	CRL validation not working for HTTPS	Internal	
6	STSI-781	Defect	Translation for "Invalid Certificate" not there in German language.	Internal	This is not a bug. After confirmation from NECPF this issue is being closed.
7	STSI-782	Defect	Held occurred if two client certificate is passes as an argument “security.ssl.8021x.client.cert" one after the other	Internal	

1.42 Open Issues

The following issues have NOT been repaired in this firmware release. ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
--	STSI-828	**DT820 does not connect to HTTPS boot server over VPN(RSA)**	External	This issue has been reported from NECECT on 6th Feb. However, this issue may be fixed by this release.
--	STSI-786	**L2TP Connect Failed" is received for ikev1 when VPN is connected from Remote location (Behind NAT)**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.

FR-903160051	STSI-836	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.
FR-903160068	STSI-831	**Customer is asking how to disable call history feature**	Maintenance Enhancement Request	This is a feature request.
FR-903160069	STSI-832	**DT7xx: Display Diversion destination i.c.o. activated diversion**	Maintenance Enhancement Request	This is a feature request.

4.1.13.16 Release

1.43 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP-v4.1 for bug fixes of VPN and 802.1X (EAP-TLS) features.

1.44 Software Release Details

Date	January 16, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.13.16	Defect Fix Release

1.45 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIP V4.1	Firmware Release	4.1.13.16	• Bug fixes for VPN and 802.1X EAP-TLS as mentioned in section 1.47 • Fix for bug FR-927160002 is removed in this release. This fix was causing issue SITD-516. Because of removal of FR-927160002 fix, SITD-516 is marked as fixed while FR-927160002 is added as known issue.	

1.46 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.47 List of Fixed Issues

1.47.1 List of Fixed Issues in STD-SIP 4.1.13.16

S No.	NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	STSI-681	Defect	[802.1X EAP-TLS] Terminal authenticates successfully even if the client certificate private key is not encrypted.	Internal	As a fix, if client certificate will contain unencrypted private key then terminal will display "**802.1X : Invalid Certificate"**
2	STSI-722	Defect	Held State occur if the private key is not encrypted If terminal's client certificate has unencrypted private key then it displays "802.1X: Held" with FreeRadius server while it displays "802.1X : Acquired" with Windows Radius Server 2012.	Internal	This is a duplicate of issue STSI-681
3	STSI-759	Defect	"Held" Observed on terminal when current time is before the start date of certificate in 802.1X. If terminal's certificates were not yet valid then terminal display "802.1X: Held" screen	Internal	As a fix, if either root/client certificates are not yet valid as per current time then terminal will display "**802.1X : Invalid Certificate"**
4	STSI-779	Defect	No error is Observed on terminal when current time is before the start date of certificate in VPN	Internal	As a fix, if either root/client certificates are not yet valid as per current time then terminal will display "**Invalid Certificate"**

5	SITD-516	Defect	([NECPF] Play ROT after transferring When the ringing transfer operation is executed on DT820, DT820 plays ROT (Reorder tone) during 5 second. The following is this operation. 1. DT820 A calls B with using handset. B is ringing. 2. B answers A. 3. A presses Transfer key. B is held and hears Hold on Music. 4. A calls C. C is ringing. 5. A puts the handset. B is transferred to C. However ROT is played during 5 second on A. [Note 1] Even if Speaker key is used instead of handset in operation 1 and 5, ROT is played on A. [Note 2] Same issue occurs in DT700 v2.3. 60.9 and DT730G v3.1.24.20.	External	This issue was introduced because of fix of FR-927160002. Fix of FR-927160002 is removed from this release hence this issue should not get reproduced.
6	STSI-720	Defect	IsValidDataValue syslog is no longer being shown in case of invalid data entry via config files.	Internal	This was an environment issue. After correcting environment, this issue was resolved.

1.48 Open Issues

The following issues have NOT been repaired in this firmware release.**ARs/BRs/ FRs and Defects, NOT Repaired**	**JIRA ID**	**Summary**	**Defect Category**	**Comments**
--	STSI-782	**Held occurred if two client certificate is passes as an argument “security.ssl.8021x.client.cert" one after the other.**	Internal	
--	STSI-781	**STD-SIP_v4.1_DQA : Translation for "Invalid Certificate" not there in German language.**	Internal	“Invalid Certificate” string’s translation is not present in “de_DE.po” file.
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI’s environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	This issue was introduced because of wpa_supplicant 2.5 upgrade. NEC-SIP firmware also shows similar behavior with wpa_supplicant 2.5.

--	STSI-763	**Terminal is unable to download config files when VPN is connected from remote location (public network)**	Internal	
--	STSI-764	**CRL validation not working for HTTPS**	Internal	
FR-903160051	SITD-492	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.
FR-927160002	SITD-496	**In the current implementation, only 503 and 580 were pulled out to play a tone (busy/reorder) in 5xx codes by phone**	Maintenance Defect	This issue was fixed in release 4.1.13.6. However fix of this issue has introduced SITD-516 hence fix of FR-927160002 has been removed from this release. This issue is now reopened.

4.1.13.6 Release

1.49 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP-v4.1 for bug fixes of VPN and 802.1X (EAP-TLS) features. WPA supplicant is also upgraded to version v2.5 in this release.

1.50 Software Release Details

Date	January 06, 2017	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.13.6	Defect Fix Release

1.51 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIP V4.1	Firmware Release	4.1.13.6	• Bug fixes for VPN and 802.1X EAP-TLS as mentioned in section 0 • Latest bug fixes of v3.1 and v4.0 are merged. • MO files are updated for above features. • WPA Supplicant is upgraded to version v2.5 • Config file was changed by FR-001160132 (Merge from v2.3)	

1.52 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.53 List of Fixed Issues

1.53.1 List of Fixed Issues in STD-SIP 4.1.13.6

S No.	Bugzilla ID (B), NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	STSI-554	Defect	The cancel key from inside the RTCP-XR Matrix takes us to DHCP instead of to RTCP-XR	Internal	
2	--	Enhancement	To support sha256 certificate, WPA Supplicant has been upgraded to v2.5	Internal	
3	STSI-651	Defect	VPN client certificate is used even if name specified in security.ssl.vpn.client.cert is incorrect.	Internal	
4	STSI-652	Defect	Error Message 802.1X:LogOff() is returned and Terminal reboots after some time when speed settings is changed from PC	Internal	
5	STSI-669	Defect	Translation not being done properly for Danish	Internal	
6	STSI-670	Defect	Translation not being done properly for French	Internal	
7	STSI-680	Defect	Terminal goes from RTCP-XR to DHCP Mode if exit key is pressed	Internal	This is duplicate of defect STSI-554
8	STSI-736	Defect	EAP Logoff message is not received when PC port is disconnected in case of EAP-MD5	Internal	
9	STSI-737	Defect	Terminal displays L2TP Connection Failure followed by VPN Disconnecting	Internal	

10	STSI-739	Defect	Held State occur If certificate is passed through cfg with comma and space separated.	Internal	
11	FR-001160132 (SITD-506)	Defect	Univerge Blue customer's phones are constantly ringing due to rouge INVITE attack from internet. DT700 responds to any INVITE received. This is causing Univerge Blue customer's phones ring constantly.	External	Merge from v2.3
12	FR-927160002 (SITD-496)	Defect	In the current implementation, only 503 and 580 were pulled out to play a tone (busy/reorder) in 5xx codes by phone. A customer in Italy has all DT730G phones. They are having a problem with certain calls that fail. The system topology consists of a 3C system and an IS3000 system connected via SIP trunk. The outside trunks are on the IS3000 side. The problem is as follows: 1- User on 3C making an outside call . 2- If the IS3000 returns a 504 Gateway Time-out, the MGC send this response to the phone and the phone terminates the call without playing any sort of tone 3- If the IS3000 returns a 502 Bad Gateway, the MGC send this response to the phone and the phone terminates the call without playing any sort of tone 4- If the IS3000 returns a 503 , the MGC sends this response to the phone and the phone plays an error tone for a second before terminating the call giving the user a chance to understand that the call errored We would like to know if this behavior can be reproduced on the DT700 phones before we escalate this to Japan. Knowing if this is consistent between all the NEC phone models is important before we escalate this issue.	External	Merge from v4.0

13	FR-927160003 (SITD-500)	Defect	If you make a call between two DT 730G phones , then answer the call, then mute both sides of the call, you will still hear low level background noise coming to originating phone. Reproduction in NECPF I tried the reproduction with DT700, DT730G and DT820. [Operation] The following steps are different from Sam-san's informed. However you will be able to confirm low noise easily. Step 1: TEL A calls TEL B with On Hook status (not use handset). Step 2: TEL B answers with handset. (With using handset, you can confirm low noise via handset.) Step 3: TEL A goes on Mute (press Mic button). And tap TEL A's mic that is located in front of TEL A with your finger. TEL B hears small noise via handset. [Result] Terminal FW version Result DT710 and DT730 2.3.57.1 Not reproduced. When I executed the above operation, I couldn't hear the noise. Also I executed same operation that Sam-san has informed. However I couldn't hear low noise in v2.3.57.1. DT730G 3.1.22.21 *Note Reproduced. I could hear low noise. DT820 4.0.22.21 *Note Same as above *Note These FW are the temporary version for FR-001160154. However the basic phone behavior is no changing from the previous official release version.	External	Merge from v4.0
14	FR-927160004 (SITD-510)	Defect	If a key is configured as a TrunkDial and is pressed the display only shows the number and not the name. Essentially the General is complaining that in the time between pressing a function key on his DSS console (DT700CG Rel 3.1.20.12)	External	Merge from v4.0

			and being connected, he sees trunk & line info in his display BUT NOT the Name label that is associated with that pressed function key. He wishes to see Name field at all times from pressing key, during call set-up, alerting and after connect, for the entire duration of the call. See also attached document. Let's take this as being the minimal requirement. What I mean to say is that as long as the Name field is displayed in the same display location thrgoughout all phases of the call as described above, then I assume it is OK if there is also additional trunk and or number information as well.		
15	FR-903160014	Defect	After transfer with a DT730 (2.3) with SRTP there's no media played. From a SIP trunk (192.168.160.20) a call is made towards 2106 (192.168.164.2). Then from the trunk the call is transferred blind to 2105 (192.168.164.26). There's one way speech after the transfer. At 192.168.164.2 does not play the received media. There's no ICMP. There are some error messages after the transfer, that could very well be related. The scenario works fine if 2 DT730G phones are used. Also in case I make the first calls towards 2105 and then transfer blind over the trunk towards 2106 it works fine too.	External .	This issue is not reproducible on STD-SIPv4.1. Hence no fix is applied for this issue in this firmware.
16	FR-903160039	Defect	Speech problems on DT-710 Sometimes there are speech problems during a connection. Its just as if the speech is not played. I took the speech from the Wireshark, then its OK. There's also no large delays so it also can't be a networks related issue. Attached a file that has been recorded. Note: Yesterday (= 8/31/2016) the our Polish	External	This issue is not reproducible on STD-SIPv4.1. Hence no fix is applied for this issue in this firmware.

			Partner - on behalf of the end- customer - requested to upgrade the ITE56047 ticket to 'Very Urgent'; for that reason the priority of the FR is upgraded to 'E'. Gerben Wennink.		

1.54 Open Issues

The following issues have NOT been repaired in this firmware release.**ARs/BRs/ FRs and Defects, NOT Repaired**	**JIRA ID**	**Summary**	**Defect Category**	**Comments**
--	STSI-720	**IsValidDataValue syslog is no longer being shown in case of invalid data entry via config files.**	Internal	
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-681	**[802.1X EAP-TLS] Terminal authenticates successfully even if the client certificate private key is not encrypted.**	Internal	
--	STSI-722	**Held State occur if the private key is not encrypted.**	Internal	

--	STSI-757	**802.1X Held(1) is displayed for 1 seconds and then get into "Waiting For LLDP"**	Internal	
--	STSI-763	**Terminal is unable to download config files when VPN is connected from remote location (public network)**	Internal	
--	STSI-764	**CRL validation not working for HTTPS**	Internal	
FR-903160051	SITD-492	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.

4.1.12.19 Release

1.55 Scope of the Delivery

DT820 Terminal firmware release of STD-SIP-v4.1 for bug fixes of VPN and 802.1X (EAP-TLS) features. NTP is also upgraded to version v4.2.8p9 in this release.

1.56 Software Release Details

Date	December 19, 2016	Release Version	Type of Release (Initial / Incremental / Defect fix)
		4.1.12.19	Defect fix

1.57 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIP V4.1	Firmware Release	4.1.12.19	• Bug fixes for VPN and 802.1X EAP-TLS as mentioned in section 0 • MO files are updated for above features. • NTP is upgraded to version v4.2.8p9.	

1.58 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".

- Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
- Client certificate must contain the unencrypted private key, hence no password is required for decryption.
- Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
- In VPN feature, IKEv1-RSA is not supported.
- IP Phone Manager does not search terminals which are connected through VPN.
- In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.

- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.
  - In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

1.59 List of Fixed Issues

1.59.1 List of Fixed Issues in STD-SIP 4.1.12.19

S No.	Bugzilla ID (B), NEC Issue ID (N), GM Issue ID , Tracker (T)	Defect/Enhancement	Defect Description	External /Internal	Remarks
1	STSI-738	Defect	**Parameter Missing on Factory Default, If changes were made from back-end.**	External	This issue was faced by NECECT during 3C admin testing. This issue was raised for 802.1X. However this has been verified for both 802.1X

					and VPN.
2	--	Enhancement	**To fix following vulnerability, ntpd 4.2.8p9 has been upgraded.** **CERT Vulnerability Note** **http://www.kb.cert.org/vuls/id/633847** **Network Time Protocol Project** **http://support.ntp.org/bin/view/Main/SecurityNotice#November_2016_ntp_4_2_8p9_NTP_Se**	External	NTP is upgraded to version v4.2.8p9.
3	STSI-747	Enhancement	**STD-SIP_v4.1_FT :When VPN IP address is provided and the same IP is received from VPN gateway, status of VPN IP address should be "Fixed"**	External	This was an enhancement requested by NECU. This is verified and close.
4	STSI-509	Defect	**An Extra "curser" is blinking while checking clientcert and rootcert subject in status**	Internal	This issue is fixed and closed.
5	STSI-518	Defect	**STD-SIP-v4.1: No failure message shown in syslog and instead of going to default value, the keep alive is disabled for character and special character input.**	Internal	After discussion with NECPF, this issue is closed as this behavior is same as for existing 'Push Server Port'. Kindly look at attached mail.  RE Regarding STSI-518 (P-1) Defect
6	STSI-648	Defect	**Wrong failure message received when NAT Traversal Port is changed.**	Internal	NTI has re-verified this issue and found this as environment issue. Therefore, no fix is required for this and this issue is closed.

7	STSI-649	Defect	**Terminal is sending EAP request to server even when the client certificate is invalid (Spoofed).**	Internal	In this bug, certificate was manually corrupted and Terminal was not getting authenticated using this certificate, It is stuck on "Held" state which is desired behavior as per latest 802.1X FSD (section#2.6.6.1). Therefore no fix is required for this issue. Hence this issue is closed.
8	STSI-664	Defect	**Dutch Translation not happening properly.**	Internal	This issue is fixed and closed.
9	STSI-665	Defect	**Translation not happening properly in Spanish.**	Internal	This issue is fixed and closed.
10	STSI-666	Defect	**Translation not happening properly in Italian.**	Internal	This issue is fixed and closed.
11	STSI-667	Defect	**802.1x not set to default config on doing factory default**	Internal	This is not an issue and expected behavior as terminal was using the parameter value from dt-<mac>-phone-sip.cfg. Therefore this issue is closed.
12	STSI-668	Defect	**Translation problem in Portugese.**	Internal	This issue is fixed and closed.
13	STSI-671	Defect	**Terminal remains UP even if the 802.1X client certificate is got expired.**	Internal	This is not an issue and occurred due to time zone difference. Later, it is

					clarified to tester and no fix is required.
14	STSI-673	Defect	**Terminal is getting Rebooted after some time (apx 1hr.) even if the terminal status is "busy"**	Internal	NTI has re-verified this issue and found environment issue due to SOHO router. Therefore, no fix is required for this. Hence this is closed.
15	STSI-721	Defect	**Local file is being overridden if VPN is enabled with an error at first and then disabled.**	Internal	This issue is fixed and closed.

1.60 Open Issues

The following issues have NOT been repaired in this firmware release.**ARs/BRs/ FRs and Defects, NOT Repaired**	**JIRA ID**	**Summary**	**Defect Category**	**Comments**
--	STSI-670	**Translation not being done properly for French.**	Internal	
--	STSI-669	**Translation not being done properly for Danish.**	Internal	
--	STSI-720	**IsValidDataValue syslog is no longer being shown in case of invalid data entry via config files.**	Internal	

--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	Internal	Initially, NTI has raised this bug with reference to NEC-SIP bug, however, it was not reproducible at NTI's environment. Currently, NTI has tries to reproduce this issue many times (10 times), however not able to reproduce it. NTI will keep on checking and if it is reproducible then NTI will plan to fix it.
--	STSI-739	**Held State occur If certificate is passed through cfg with comma and space separated.**	Internal	
--	STSI-736	**STD-SIP_v4.1_RT : EAP Logoff message is not received when PC port is disconnected in case of EAP-MD5**	Internal	
--	STSI-681	**[802.1X EAP-TLS] Terminal authenticates successfully even if the client certificate private key is not encrypted.**	Internal	
--	STSI-651	**VPN client certificate is used even if name specified in security.ssl.vpn.client.cert is incorrect.**	Internal	
FR-927160002	SITD-496	**In the current implementation, only 503 and 580 were pulled out to play a tone (busy/reorder) in 5xx codes by phone**	Maintenance Defect	This fix will be included after being fixed in v3.1 and v4.0.
FR-927160003	SITD-500	**Mute issue with all NEC DT phones models**	Maintenance Defect	Same as above
FR-903160014	SITD-508	**After transfer with a DT730 (2.3) with SRTP there's no media played**	Maintenance Defect	Same as above

FR-001160132	SITD-506	**DT700 rings for any INVITE not from MGC**	Maintenance Defect	Same as above
FR-903160051	SITD-492	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.
FR-927160004	SITD-510	**If a key is configured as a TrunkDial and is pressed the display only shows the number and not the name**	Maintenance Defect	This fix will be included after being fixed in v3.1 and v4.0.

4.1.12.1 Release

1.61 Scope of the Delivery

DT820 Terminal firmware alpha release of STD-SIP-v4.1 for VPN and 802.1X (EAP-TLS) features. Sanity Testing is also executed on this release.

1.62 Software Release Details

Date	December 01, 2016	**Release Version**	**Type of Release (Initial / Incremental / Defect fix)**
		4.1.12.1	Alpha Release

1.63 Details

SN	Deliverable (File Name)	Description	Version	Change Description (Defect ID / MR ID etc.)	Remarks
1	STD-SIP V4.1	Firmware Release	4.1.12.1	Alpha Release firmware for following features: • VPN • 802.1X Configuration Files and MO files are updated for above feature.	

1.64 Notice

- **VPN Feature**
  - User must configure VPN parameters in configuration file which are mentioned in VPN's FSD. All configurations must be done at central site.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the VPN certificates on the terminal before enabling RSA authentication at remote side. This could be done either by PSK authentication at the remote side or by disabling VPN at the central site.
  - Client certificate must contain the unencrypted private key, hence no password is required for decryption.
  - Central Site DNS server is not supported. Therefore, all the server addresses must be given in IP address format. Domain name should not be used. This will be added as limitation in VPN's FSD.
  - In VPN feature, IKEv1-RSA is not supported.
  - IP Phone Manager does not search terminals which are connected through VPN.
  - On 29th Nov, the following change has been requested from NECU.

  This change isn't included in this release, and will be included in December or January's release before GA.
  [Change Request]
  VPN IP address display of the fixed IP is changed from "xxx.xxx.xxxx.xxx" to "xxx.xxx.xxxx.xxx(Fixed)".
  - In development environment, CISCO 881-k9, with FW v15.4 (3) M5, was used in testing.
- **802.1X (EAP-TLS) Feature**
  - User must configure 802.1X (EAP-TLS) parameters in configuration file which are mentioned in 802.1X (EAP-TLS)'s FSD.
  - Supported certificate format is "PEM" with following file extensions ".crt", ".pem", ".cer", and ".key".
  - Please download the 802.1X (EAP-TLS) certificates on the terminal before enabling EAP-TLS. This could be done either by disabling 802.1X feature or enabling 802.1X MD5 with correct user name and password.
  - Client certificate must contain the encrypted private key and its password must be given through "security.ssl.8021x.client.certpassword" parameter of config file.
  - Client certificate CN must be configured in EAP-TLS username.

- In development environment, Windows Server 2012 R2 as Radius server and FreeRADIUS.net-1.1.7-r0.0.2 is used in testing.

- **Translation Testing**
  - Almost translations for v4.1 are included in MO files. However some translations (Brazilian and some translation of “Dynamic” and “Fixed”) aren’t included. These translation will be included in later release.
  - Language related testing is in-progress, so there could be some issues related to STD-SIP-v4.1 text strings.

1.65 List of Fixed Issues

1.65.1 List of Fixed Issues in STD-SIP 4.1.12.1

None

1.66 Open Issues

The following issues have NOT been repaired in this firmware release.

ARs/BRs/FRs and Defects, NOT Repaired	JIRA ID	Summary	Defect Category	Comments
--	STSI-648	**wrong failure message received when NAT Traversal Port is changed**	VPN Feature Defect	This could be an environment issue and may not require code changes. NTI will check and close after confirmation.
--	STSI-628	**When IKE version is IKEV2 and Authentication Mode is RSA after rekeying VPN connection gets disconnected**	VPN Feature Defect	This issue is same as NEC-SIP. Please refer DT800 Firmware Release Note(V93.0.10.0).xlsx

--	STSI-518	**STD-SIP-v4.1: No failure message shown in syslog and instead of going to default value, the keep alive is disabled for character and special character input.**	VPN Feature Defect	This is a minor GUI issue. NTI will fix it after Alpha release.
--	STSI-673	**STD-SIP-v4.1_IT :Terminal is getting Rebooted after some time (apx 1hr.) even if the terminal status is "busy"**	VPN Feature Defect	This is raised on 30th Nov, therefore need to analyze it.
--	STSI-649	**STD-SIP_v4.1_FT : Terminal is sending EAP request to server even when the client certificate is invalid (Spoofed).**	802.1X (EAP-TLS) Feature Defect	This issue may not occur at customer side as certificate hashing was changed manually. As a result "Network Status" displays client certificate name but certificate's other information is displayed as "Not Available" as certificate is corrupted. Please note that 802.1X authentication through EAP-TLS will not be possible with this certificate and terminal will remain stuck on "Held" case which is the expected behavior
--	STSI-509	**STD-SIP-v4.1: An Extra "curser" is blinking while checking clientcert and rootcer subject in status.**	802.1X (EAP-TLS) Feature Defect	This is a minor GUI issue. NTI will fix it after Alpha release.
--	STSI-671	**STD-SIP-v4.1__IT : Terminal remains UP even if the 802.1X client certificate is Got expired**	802.1X (EAP-TLS) Feature Defect	This is raised on 30th Nov, therefore NTI need to analyze it.

--	STSI-667	**802.1x not set to default config on doing factory default**	802.1X (EAP-TLS) Feature Defect	This is raised on 30th Nov, therefore NTI need to analyze it.
FR-927160002	SITD-496	**In the current implementation, only 503 and 580 were pulled out to play a tone (busy/reorder) in 5xx codes by phone**	Maintenance Defect	This fix will be included after being fixed in v3.1 and v4.0.
FR-927160003	SITD-500	**Mute issue with all NEC DT phones models**	Maintenance Defect	Same as above
FR-903160014	SITD-508	**After transfer with a DT730 (2.3) with SRTP there's no media played**	Maintenance Defect	Same as above
FR-001160132	SITD-506	**DT700 rings for any INVITE not from MGC**	Maintenance Defect	Same as above
FR-903160051	SITD-492	**DT7xx/DT8xx Should not accept digits after cancel of second call**	Maintenance Enhancement Request	This is a feature request.

1.67 Installation Requirements

The v4.1 release file contains DT820 Terminal Firmware. Extract the contents from this file and place them in the Boot Server. The v4.1 release file contains

1. ityissipe.tgz
2. ityissipex.tgz
3. ityissipe.sig
4. ityissipex.sig
5. MO Files
6. Default Config Files
7. Wav Files
8. Necsdt820.ver file
9. 3CtoDT700languagemappings.txt

Note: On 3C place the above files in “necsdt700” folder under “ftproot”

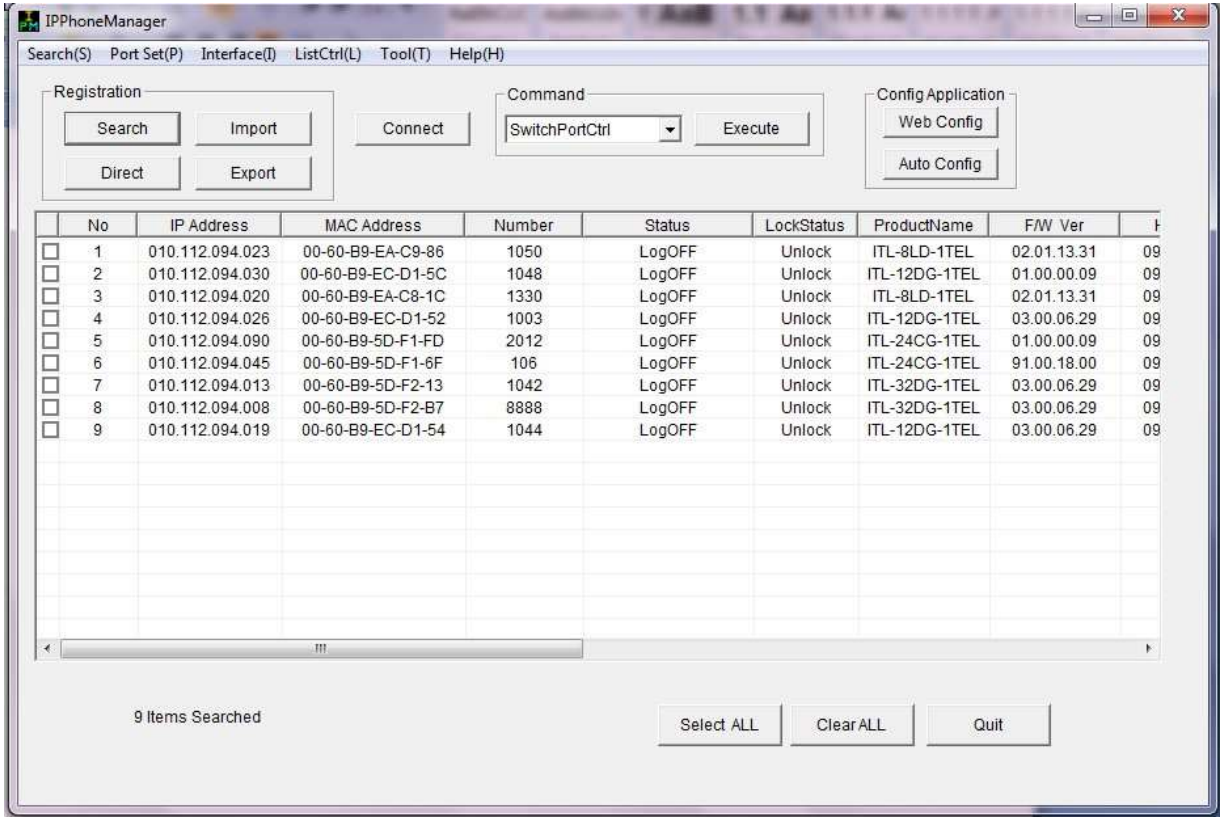
The following are ways to download Lynx Firmware to DT820 NEC-SIP Firmware:

Using IP Phone Manager

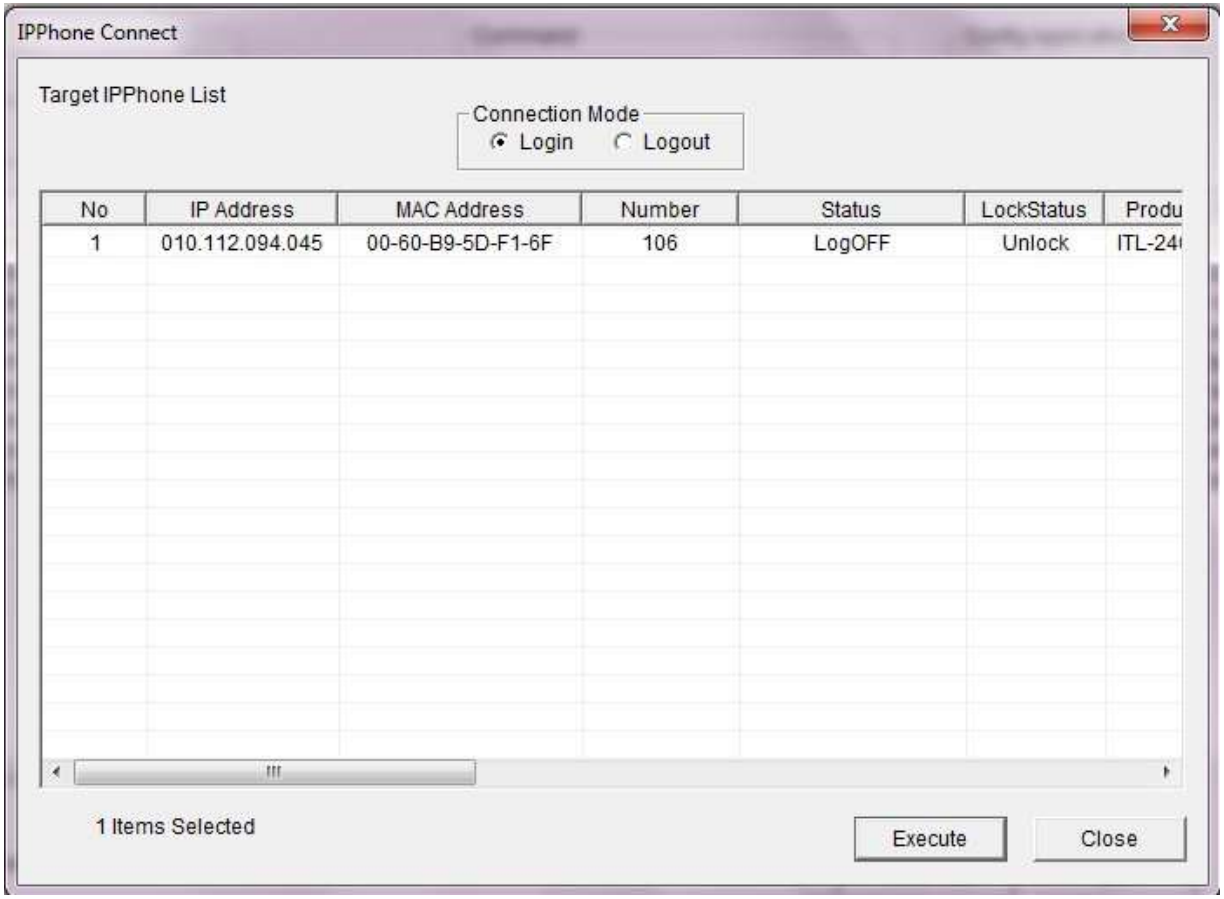
IP Phone Manager Version 8.2.0 or later supports conversion from NEC-SIP to Lynx firmware and vice-versa. The firmware conversion from NEC-SIP to STD-SIP on a DT820 Terminal requires a Lynx firmware to be placed on FTP/TFTP Server.

The steps for downloading the firmware through IP Phone Manager are: *(The pictures are used from DT730G and will be replaced in later release)

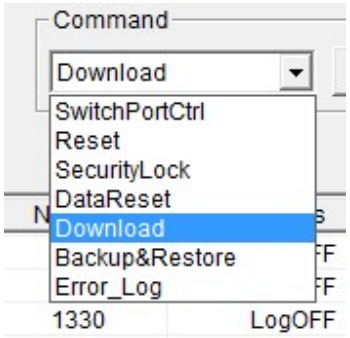
1. Search list of the active Terminals as shown in the figure below.



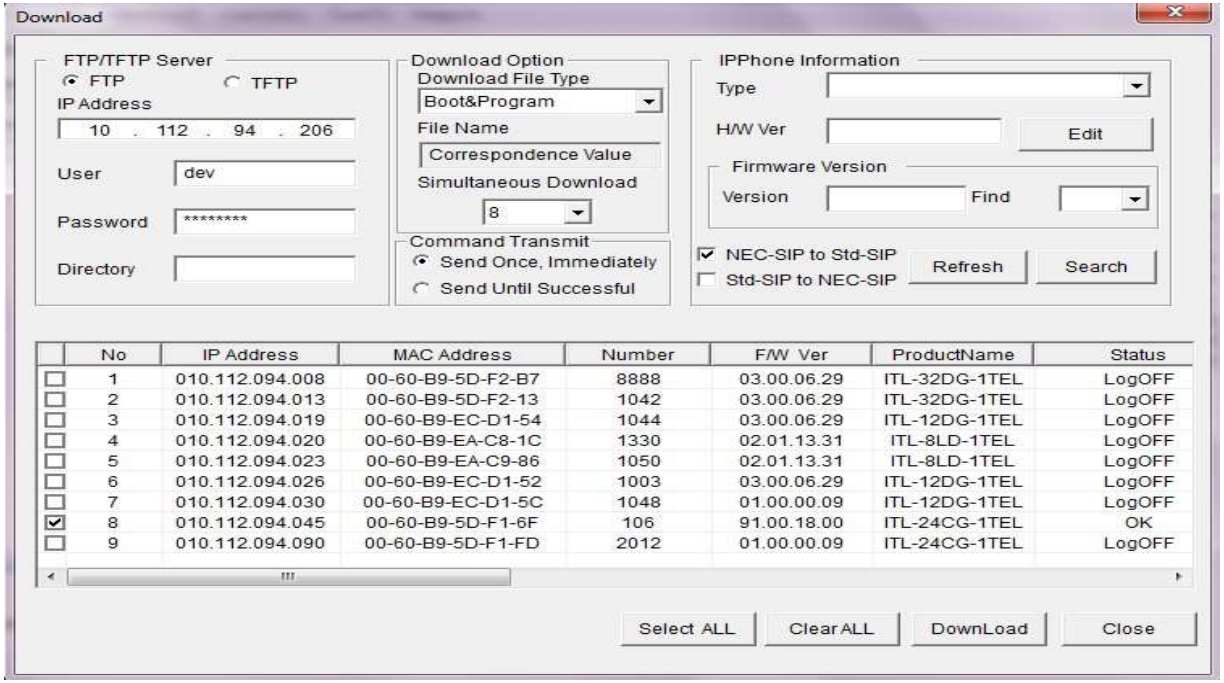
2. Select the Terminal on which the conversion is to be done and press “Connect” to get connected with terminal. After this step terminal will get connected with IP Phone Manager as shown below.



3. After the Terminal gets connected, choose the **download** option under the command drop-down menu.



Click on Execute. The following window will pop up



4. Depending upon the Server type FTP or TFTP, the type can be specified in the above screen

   a. FTP/TFTP Server:Select the type of server - FTP or TFTP.
      Define the IP address of the server.
      Enter the User ID (*FTP Only)*.
      Enter the Password (*FTP Only)*.
      Enter the Directory name (*FTP Only)*.

   b. Use the Download Option Field to select the Terminal File type and enter the File type as "**Boot&Program"**.

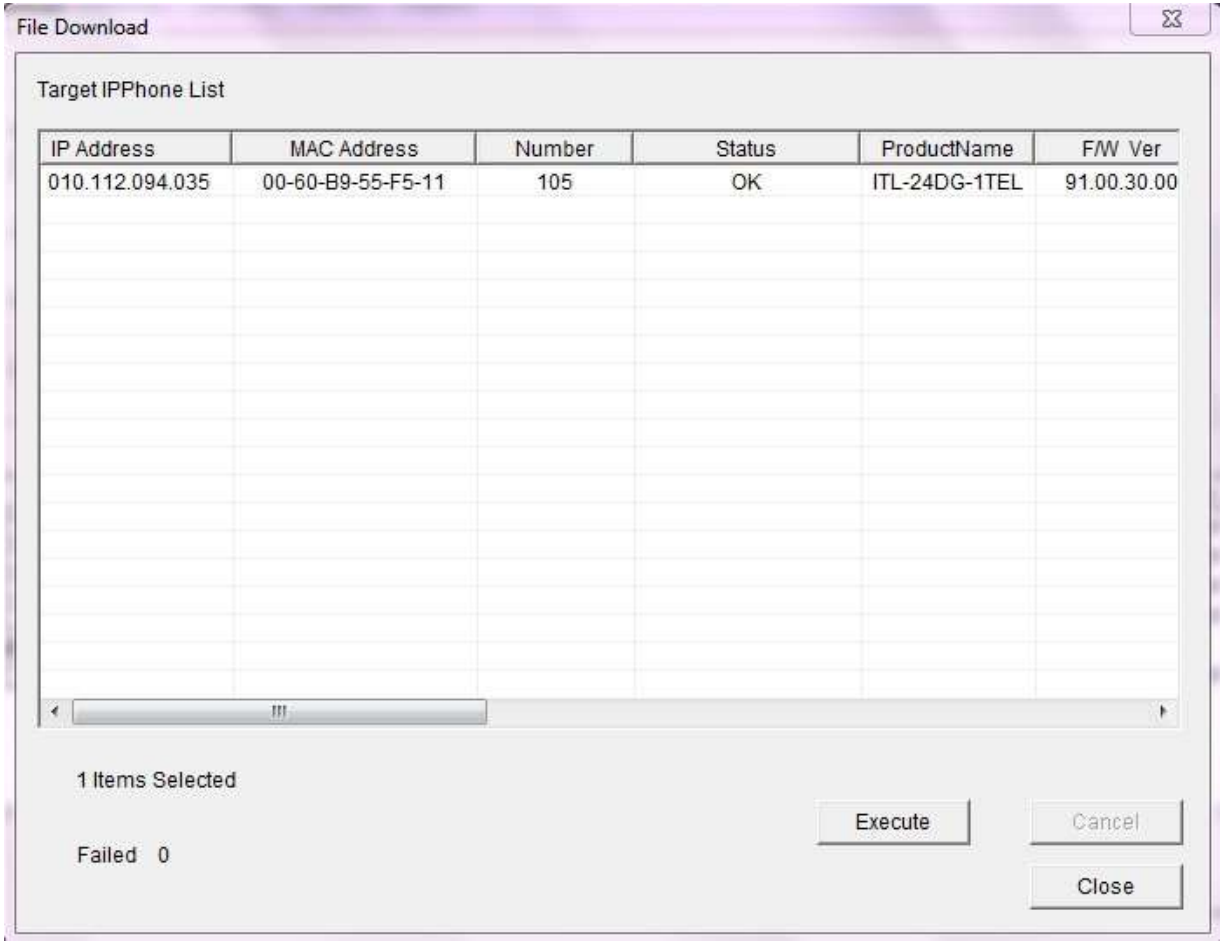
   c. Under IP Phone Information specify the Type of IP Phone .While converting the firmware from NEC-SIP to STD-SIP, the type to be specified is:

   d. Specify the Firmware version (if required)

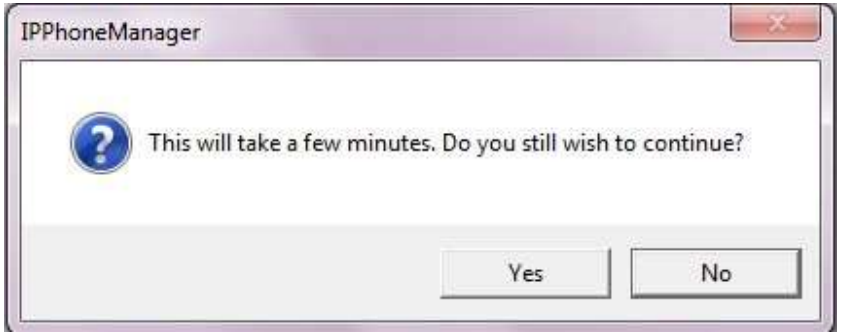
   e. Select the check box for NEC-SIP to STD-SIP for conversion for NEC-SIP to STD-SIP firmware conversion.

   After the above steps, click on "Download"

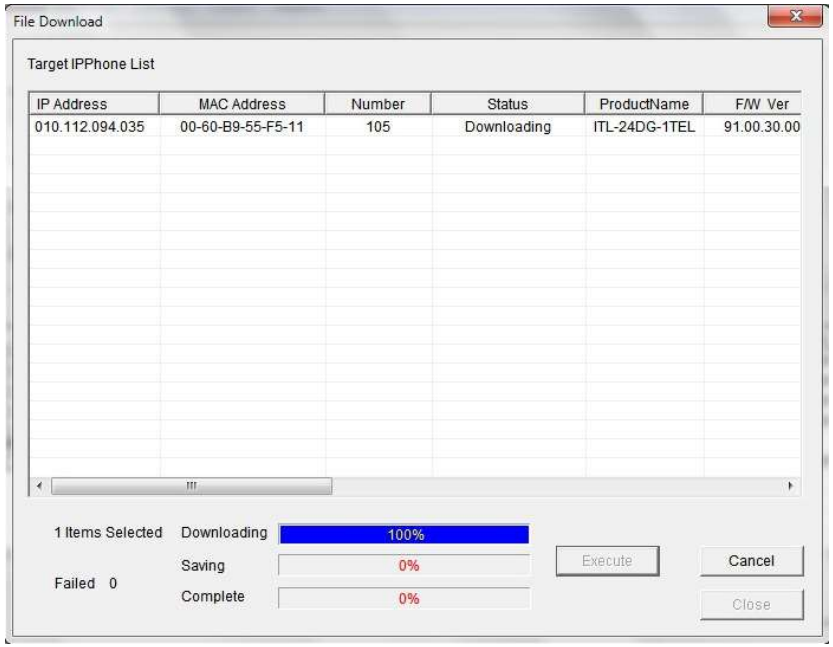
5. The following pop-up window will be displayed .Press Execute to begin the Download process.

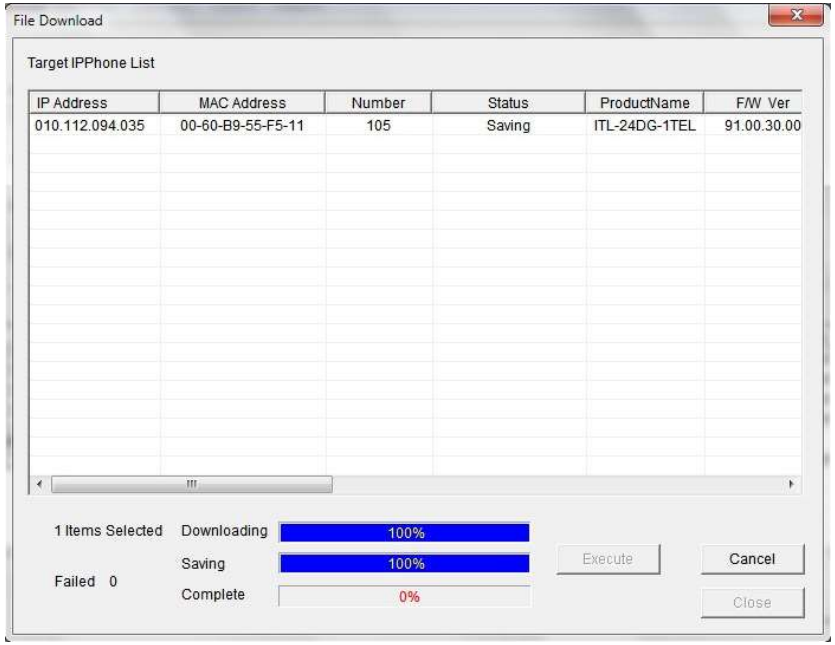


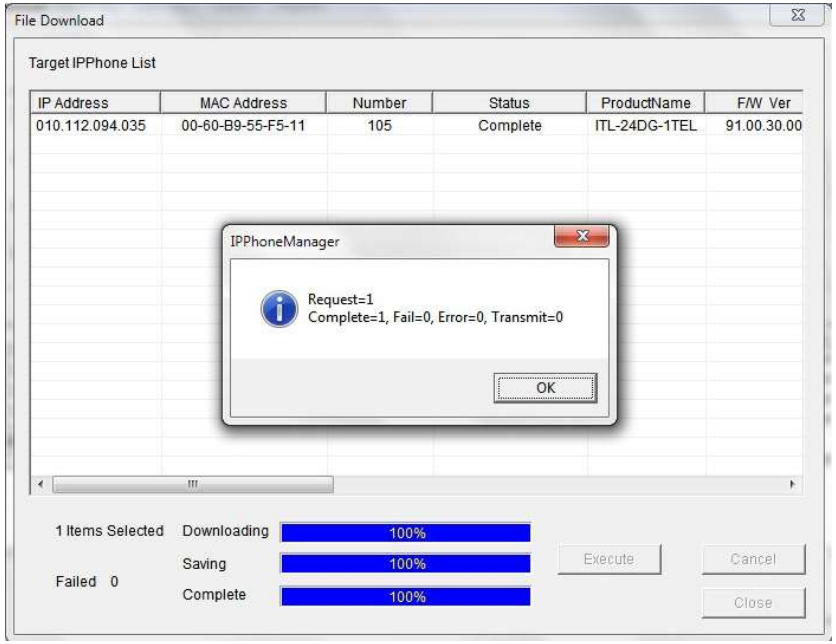
6. On Pressing Execute, the following dialogue will appear...



7. Press “Yes” which triggers the download process. The following screens will come up.




File Download
Target IPPhone List
IP Address
MAC Address
Number
Status
ProductName
F/W Ver
010.112.094.035
00-60-B9-55-F5-11
105
Saving
ITL-24DG-1TEL
91.00.30.00
1 Items Selected
Downloading
100%
Saving
100%
Failed 0
Complete
0%
Execute
Cancel
Close



8. The above screen shows that the Firmware has been Downloaded